



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,560	02/09/2004	Young-Hyun Kim	678-1163	1111
66547 7590 09/12/2008 THE FARRELL LAW FIRM, P.C. 333 EARLE OVINGTON BOULEVARD SUITE 701 UNIONDALE, NY 11553			EXAMINER PEARSON, DAVID J	
			ART UNIT 2137	PAPER NUMBER
			MAIL DATE 09/12/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/774,560	Applicant(s) KIM, YOUNG-HYUN	
	Examiner DAVID J. PEARSON	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 July 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4,6-10 and 12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4,6-10 and 12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

1. Claims 1, 4 and 8 have been amended. Claims 3, 5 and 11 have been canceled. Claims 1-2, 4, 6-10 and 12 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/02/2008 has been entered.

Claim Objections

3. Claims 6 and 12 are objected to because of the following informalities:

Claim 6 depends on claim 5. Claim 12 depends on claim 11. However, claims 5 and 11 have been canceled. Examiner believes claim 6 should depend on claim 4 and claim 12 should depend on claim 8 and will treat the claims as such for the remainder of the Office Action.

Appropriate correction is required.

Response to Arguments

4. Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-2, 4, 6-10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harada et al. (U.S. Patent Application Publication 2003/0007640) and further in view of Horiuchi et al. (U.S. Patent Application Publication 2003/0009667), Skinner (U.S. Patent Application Publication 2004/0202291) and Ginter et al. (U.S. Patent Application Publication 2002/0048369).

For claim 1, Harada et al. teach a mobile communication terminal for providing mobile communication functions, for accessing a content server by at least one of wired and wireless communication, downloading content from the content server, and uploading the downloaded content to an external device, the mobile communication terminal comprising:

A memory for storing model information and a serial number of the mobile communication terminal (note paragraphs [0102]-[0103]) and the downloaded content (note paragraph [0105]);

A communication unit for providing mobile communication functions (note paragraph [0095]) and an interface for exchanging data with the external device (note paragraphs [0123]-[0125]);

An encryption unit for encrypting the serial number and the content with the encryption key (note paragraphs [0159]-[0165]), thereby restricting use of the content to the mobile communication terminal (note paragraph [0007]);

A controller for uploading the encrypted content from the mobile communication terminal to the external device via the communication unit (note paragraph [0167]), and for transmitting a download request signal for the uploaded content to the external device in response to an input command (note paragraph [0169]); and

A decryption unit for decrypting, with the encryption key, the content downloaded from the external device in response to the download request signal for the uploaded content (note paragraph [0174]).

Harada et al. differ from the claimed invention in that they fail to specify:

A memory also for storing an encryption key for encrypting the content downloaded from the external device.

Horiuchi et al. teach:

A memory also for storing an encryption key for encrypting the content downloaded from the external device (note paragraphs [0109] and [0114]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the content storage device of Harada et al. with the memory card that generates an encryption key for the mobile terminal of Horiuchi et al. One of

ordinary skill in the art at the time of the invention would have been motivated to combine Harada et al. and Horiuchi et al. because it would improve the security of transmitting data between the mobile device and the external device (note paragraph [0072] of Horiuchi et al.).

The combination of Harada et al. and Horiuchi et al. differ from the claimed invention in that they fail to specify:

An external device which is not attached to the mobile communication terminal.

Skinner teaches:

An external device which is not attached to the mobile communication terminal (note paragraphs [0042] and [0078]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Harada et al. and Horiuchi et al. and the wireless transmission of Skinner. It would have been obvious to substitute the wireless transmission of Skinner for the removable memory card of the Harada et al. and Horiuchi et al. combination because it would yield the predictable results of transferring encrypted contents to a target device.

The combination of Harada et al., Horiuchi et al. and Skinner differs from the claimed invention in that they fail to teach:

Wherein the encryption key is generated by the external device considering further time information set in the external device.

Ginter et al. teach:

Wherein the encryption key is generated by the external device considering further time information set in the external device (note paragraph [1648]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Harada et al., Horiuchi et al. and Skinner and the time based keys of Ginter et al. One of ordinary skill in the art at the time of the invention would have been motivated to combine Harada et al., Horiuchi et al., Skinner and Ginter et al. because it would allow the sender and receiver to generate a common secret key without potentially compromising its security by communicating it over an insecure channel (note paragraph [1640] of Ginter et al.).

For claim 4, the combination of Harada et al., Horiuchi et al., Skinner and Ginter et al. teaches a content security system comprising:

A mobile communication terminal for providing mobile communication functions (note paragraph [0091] of Harada et al.), for encrypting content provided from a content server (note paragraph [0165] of Harada et al.) with an encryption key provided from an external device (note paragraph [0109] of Horiuchi et al.) which is not attached to the mobile communication terminal (note paragraphs [0042] and [0078] of Skinner), and for

uploading the encryption content from the mobile communication terminal to the external device (note paragraph [0167] of Harada et al.); and

An external memory device for generating the encryption key based on model information and a serial number of the mobile terminal (note paragraph [0103] of Harada et al.), and storing the encrypted content uploaded from the mobile communication terminal (note paragraph [0155] of Harada et al.), **wherein the external memory device generates the encryption key considering further time information set in the external memory device** (note paragraph [1648] of Ginter et al.).

For claim 8, the combination of Harada et al., Horiuchi et al., Skinner and Ginter et al. teaches a content protection method using a content security system having a mobile communication terminal for providing mobile communication functions and downloading content from a content server and an external memory device for storing the content at a request of the mobile communication terminal, the external memory device not being attached to the mobile communication terminal (note paragraphs [0042] and [0078] of Skinner), the method comprising the steps of:

Transmitting a content upload request signal from the mobile communication terminal to the external memory device in response to an input command (note paragraph [0181] of Harada et al.);

Transmitting to the external memory device model information and a serial number of the mobile communication terminal, requested by the external memory

device in response to the content upload request signal (note paragraph [0103] of Harada et al.);

Encrypting content to be uploaded from the mobile communication terminal (note paragraph [0181] of Harada et al.) with an encryption key generated by the external memory device (note paragraph [0109] of Horiuchi et al.) based on the model information and the serial number (note paragraph [0103] of Harada et al.); and

Transmitting the content encrypted by the encryption key from the mobile communication terminal to the external memory device (note paragraph [0181] of Harada et al.), **wherein the encryption key is generated by the external device considering further time information set in the external device** (note paragraph [1648] of Ginter et al.).

For claim 2, the combination of Harada et al., Horiuchi et al., Skinner and Ginter et al. teaches claim 1, wherein the encryption key is generated by the external device (note paragraph [0109] of Horiuchi et al.) based on the model information and the serial number of the mobile terminal (note paragraph [0103] of Harada et al.).

For claims 6 and 12, the combination of Harada et al., Horiuchi et al., Skinner and Ginter et al. teach claims 5 and 11, wherein the external memory device determines whether the time information set in the external memory device is identical to time information set in the mobile communication terminal, and generates the encryption key

if the time information set in the external memory device is identical to time information set in the mobile communication terminal (note paragraph [0520] of Ginter et al.).

For claim 7, the combination of Harada et al., Horiuchi et al., Skinner and Ginter et al. teaches claim 4, wherein the mobile communication terminal transmits a download request signal for previously uploaded content to the external memory device in response to an input command, and decrypts, with the encryption key, content downloaded from the external memory device in response to the download request signal (note paragraph [0184] of Harada et al.).

For claim 9, the combination of Harada et al., Horiuchi et al., Skinner and Ginter et al. teaches claim 8, further comprising the steps of:

Determining whether the encrypted content uploaded from the mobile communication terminal is identical to the content encrypted by the encryption key (note paragraph [0307] of Harada et al.); and

Storing the encrypted content on the external memory device is the encrypted content uploaded from the mobile communication terminal is identical to the content encrypted by the encryption key (note paragraph [0319] of Harada et al.).

For claim 10, the combination of Harada et al., Horiuchi et al., Skinner and Ginter et al. teaches claim 9, further comprising the steps of:

Upon receiving a download command from the previously uploaded content, transmitting a content download request signal from the communication terminal to the external memory device (note paragraph [0183] of Harada et al.);

If content index information for downloading is selected from content index information provided from the external memory device in response to the content download request signal, transmitting the selected content index information to the external memory device (note paragraph [0124] of Horiuchi et al.);

If encrypted content is downloaded from the external memory device according to the selected content index information, decrypting the downloaded encrypted content with the encryption key (note paragraph [0184] of Harada et al.).

Response to Arguments

6. Applicant argues Horiuchi fails to teach use of content restricted to the mobile communication device which obtained the content and therefore fails to supplement the deficiencies of Harada (note Remarks, page 7).

Examiner disagrees. Horiuchi was not relied upon to teach use of content restricted to the mobile communication device which obtained the content. Harada teaches content being restricted to a particular mobile device.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

Art Unit: 2137

USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant argues modifying Harada with Horiuchi would result in an encryption unit that would not restrict use of the content to the mobile communication device and would destroy the configuration of Harada (note Remarks, pages 7-8).

Examiner disagrees. Harada teaches a key based on the unique phone information (note paragraph [0162]). Horiuchi teaches a memory card (external device) that sends a key to a phone for performing encryption (note paragraph [0109]). Therefore, the combination of Harada and Horiuchi teaches an external device generating a key based on a phone's unique information sending it to the phone for using in encryption.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Matsuzaki et al. (U.S. Patent Application Publication 2001/0056541) teaches key generation based on the current time to encrypt a file (note paragraph [0054]).

Kuriya et al. (U.S. Application Publication 2001/0056404) teaches a mobile telephone receiving and storing a content key (note paragraph [0203]).

Hori (U.S. Application Publication 2002/0136405) teaches a decryption key unique to the class of decrypting unit (note paragraph [0077]).

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID J. PEARSON whose telephone number is (571)272-0711. The examiner can normally be reached on Monday - Friday, 7:30am - 5:00pm; off every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DJP

Application/Control Number: 10/774,560
Art Unit: 2137

Page 13

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137